

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

平4-149690

⑬ Int.Cl.⁵

識別記号

庁内整理番号

⑭ 公開 平成4年(1992)5月22日

G 06 K 17/00

S

6711-5L

G 07 F 7/08

G 07 G 1/12

3 2 1 P

8921-3E

8111-3E

8111-3E

G 07 F 7/08

C

M

審査請求 未請求 請求項の数 1 (全7頁)

⑮ 発明の名称 記録データ処理装置

⑯ 特 願 平2-271462

⑰ 出 願 平2(1990)10月9日

⑱ 発 明 者 大 石 和 弘 東京都西多摩郡羽村町栄町3丁目2番1号 カシオ計算機株式会社羽村技術センター内

⑲ 出 願 人 カシオ計算機株式会社 東京都新宿区西新宿2丁目6番1号

明 細 書

1. 発明の名称

記録データ処理装置

2. 特許請求の範囲

入力される暗号データを設定自在に記憶する暗号データ記憶手段と、この暗号データ記憶手段に記憶された暗号データに基づき、記録媒体のデータを暗号化あるいは復号化して記録媒体に対して読み書きする読み書き手段と、各種命令に従って各種処理を実行する実行制御手段と、各種命令が正常命令か否かを判別する判別手段と、この判別手段で各種命令が正常命令でないと判別された際に上記暗号データ記憶手段に記憶された暗号データを消去する消去手段とを具備したことを特徴とする記録データ処理装置。

3. 発明の詳細な説明

〔産業上の利用分野〕

この発明は、例えばプリペイドカードリーダー・ライタ等の記録データ処理装置に関する。

〔従来の技術〕

ECRやPOSターミナル等に接続されるプリペイドカードリーダー・ライタは、暗号化・復号化ルーチンプログラムをROMに記憶し、プリペイドカードに対して読み込み、暗号データの復号、金額減算、暗号化、書き込み、という処理を行なうものであった。

〔発明が解決しようとする課題〕

そのため、プリペイドカードリーダー・ライタを盗んでROMプログラムを解析して、プリペイドカードに金額データを書き込む命令コードを探り当て、不正にプリペイドカードを発券するという犯罪が発生している。

この発明の課題は、プリペイドカードリーダー・ライタが盗難にあっても、プリペイドカードが不正に発券されることを防止できるようにすることである。

〔課題を解決するための手段〕

この発明の手段は次の通りである。

暗号データ記憶手段1(第1図の機能ブロック図を参照、以下同じ)は、例えばRAMにより構

成され、入力される暗号データを設定自在に記憶する。

読み書き手段2は、例えば磁気カードリーダー・ライター等であり、暗号データ記憶手段1に記憶された暗号データに基づき、磁気カード等の記録媒体のデータを暗号化あるいは復号化し、記録媒体に対して読み書きする。

実行制御手段3は、各種命令に従って各種処理を実行する。

判別手段4は、各種命令が例えばROMに記憶された正常命令か否かを判別する。

消去手段5は、判別手段4で各種命令が正常命令でないと判別された際に上記暗号データ記憶手段1に記憶された暗号データを消去する。

〔作用〕

この発明の手段の作用は次の通りである。

暗号データ記憶手段1に記憶された暗号データに基づいて読み書き手段2が記録媒体のデータを暗号化・復号化し、磁気カード等の記録媒体に対して読み書きし、実行制御手段3が各種命令に従

って各種処理を実行する。

判別手段4で各種命令が正常命令でないと判別された際に、消去手段5は上記暗号データ記憶手段1に記憶された暗号データを消去する。

従って、プリペイドカードリーダー・ライターが盗難にあい、プリペイドカードに対して不正にデータを書き込もうとしても、異なる命令が指示された際に暗号データが消去されるので、プリペイドカードに正規のデータを書き込めず、プリペイドカードが不正に発券されることを防止できる。

〔実施例〕

以下、実施例を第2図乃至第5図に示す図面に基づいて説明する。なお、この実施例はプリペイドカードリーダー・ライターにより構成された記録データ処理装置を示している。

第2図は、プリペイドカード端末装置の回路構成を示すブロック図である。このプリペイドカード端末装置は例えばECRである。

同図において、鉤入力装置10は図示しないが「0」～「9」等の数値データを入力するテンキー、

各種処理を指定するファンクションキー、売上データの部門別登録を指定する部門キー、各モードを指定するモードキー、およびその他のキーを備えている。しかして、鉤入力装置10はキー入力を行なうと、これに応じたキー入力信号をCPU11に出力する。

CPU11は、鉤入力装置10から出力されるキー入力信号に応じて登録処理、定額引落し処理等の各種処理を実行する。これらの各種処理はROM12に予め記憶した制御プログラムに基づいて実行される。

RAM13は各種データを記憶するもので、CPU11により読出し／書き込みが制御される。プログラムカード1／F（インターフェイス）14は、プログラムカード15とCPU11とのデータ授受を行なう。プログラムカード15は、暗号データを記憶したROMカードまたはRAMカードにより構成されている。リーダー・ライター1／F16はプリペイドカードリーダー・ライター17とCPU11とのデータ授受を行なう。表示部18は

例えば蛍光表示パネルにより構成されるもので、CPU11から出力される表示データを表示する。プリンタ19はCPU11から出力される印字データを印字する。

第3図は、プリペイドカードリーダー・ライター17の回路構成を示すブロック図である。このプリペイドカードリーダー・ライター17は、例えば磁気カードにより構成されるプリペイドカードに対して金額データの読み込み及び書き込みを行なうものである。同図において、CPU20は図示しない内部ROMに記憶した制御プログラムに基づいて各部を制御するもので、リーダー・ライターメカニズム21、ROM22、RAM23、およびI／F24が接続されている。

リーダー・ライターメカニズム21は、プリペイドカードに記録されたデータを読み込み又は書き込むための磁気ヘッド、カード搬送機構等を内蔵するものである。この場合、プリペイドカードにはカード種類、発行番号、金額データ等のデータが記録されている。

ROM 22には、例えば第3図に示すように暗号ダウンロードコマンド、読み込みコマンド、書き込みコマンド、エジェクトコマンド、および暗号ルーチン等の各種制御情報が予め記憶されている。この実施例において、暗号ダウンロードコマンドはプリペイドカード端末装置から送信された暗号データをRAM 23のエリアにセーブすることを指示するコマンドである。読み込みコマンドは、プリペイドカードのデータを読み込んで暗号化して送信することを指示するコマンドである。書き込みコマンドは、プリペイドカードに金額データを書き込むことを指示するコマンドである。エジェクトコマンドは、プリペイドカードを装置の外に排出することを指示するコマンドである。暗号ルーチンは、RAM 23に記憶された暗号データに基づいてプリペイドカードに書き込むデータを暗号化し、或いはプリペイドカードから読み込んだ暗号化されたデータを元のデータに復号化するためのプログラムである。

RAM 23は、プリペイドカード端末装置から

ラムカード15がI/F 14と接続されているか否かが判断される。プログラムカードが有る場合は、ステップA2でYESと判断されてステップA3に進む。もし、プログラムカードがない場合はNOとなり、ステップA8によりエラー表示が実行されてステップA1に戻る。

ステップA3においては、プログラムカード15に記憶された暗号データがI/F 14を介してCPU 11に読み出される。続くステップA4では、プログラムカード15から読み出された暗号データと暗号ダウンロードコマンドとをI/F 18を介してプリペイドカードリーダー・ライター7に転送する。

次に、ステップA5ではデータが正常に転送されたか否かが判断され、正常であればステップA6に進み、正常でなければステップA9のエラー表示に進む。

ステップA6においては、プリペイドカードリーダー・ライター7に対して読み込みコマンドを送信し、読み込みコマンドに応じてプリペイドカー

初期設定時にセーブされた暗号データを記憶するもので電池23aから記憶保持のための電源が供給されている。

I/F 24はプリペイドカード端末装置と接続されてデータ通信を行なうものである。

次に、第4図および第5図に示すフローチャートに基づき上記実施例の動作を説明する。

第4図を参照してプリペイドカード端末装置の動作を説明する。まず、ステップA1ではINIT SW（イニシャライズ・スイッチ）が操作されたか否かが判断される。INIT SWは、プログラムカード15に記憶された暗号データをプリペイドカードリーダー・ライター7に転送してRAM 23にセーブして初期化する際に操作するスイッチである。このステップA1でYESと判断された場合はステップA2に進み、NOの場合はステップA8に進む。

ここで、プリペイドカードリーダー・ライター7を初期化するためにINIT SWを操作したとする。これにより、ステップA2に進み、プログ

ドリーダー・ライター7から送信される結果データを受信する。この場合、金額データが入力されていないので読み込みコマンドは送信されない。

ステップA7では読み込みが未完か否かが判断される。このステップA7で、読み込みが未完でYESと判断された場合はステップA1に戻り、NOの場合はステップA10に進む。この場合、読み込みコマンドを送信していないのでYESと判断されてステップA1に戻る。

次に、プリペイドカードから金額データを引落とす場合は、INIT SWをOFFしておき、制入力装置10により金額データを入力する。これにより、ステップA1でNOと判断されてステップA6に進む。

ステップA8においては、プリペイドカードリーダー・ライター7に対して読み込みコマンドを送信して残高データの読み込みを指示し、送信されてくる残高データを受信する。

ステップA7ではプリペイドカードリーダー・ライター7からの読み込みが未完か否かが判断され

る。このステップA7で、YESと判断された場合はステップA1に戻り、NOの場合はステップA10に進む。

ステップA10では、プリペイドカードリーダー・ライタ17から送信されたデータが正常な復号化データか否かが判断される。即ち、残高データを暗号データに基づいて解析し、正常な復号化データか否かを判断する。このステップA10でYESと判断されるとステップA11に進み、NOの場合はステップA15のエラー表示に進む。

ステップA11においては、残高データから売上データを減算することが可能か否かが判断される。ステップA11でYESと判断されるとステップA12に進み、残高データが売上データよりも小さくNOと判断されるとステップA15のエラー表示に進む。

ステップA12では、プリペイドカードの残高データから売上データを減算し、減算後の残高データと書き込みコマンドとを送信して残高データの書き込みを指示し、プリペイドカードリーダー・

ライタ17から送信されてくる結果OKデータを受信する。

ステップA13では正常書き込み完了か否か、即ちプリペイドカードリーダー・ライタ17が結果OKデータを送信したか否かが判断される。このステップA13でYESと判断された場合はステップA14に進み、NOの場合はステップA15に進む。

ステップA14において、プリペイドカードリーダー・ライタ17に対してカードエジェクトコマンドを送信し、ステップA1に戻る。

次に、第5図を参照してプリペイドカードリーダー・ライタ17の動作を説明する。

ステップB1では、プリペイドカード端末装置からのコマンドを受信したか否かが判断される。コマンドを受信していない場合はステップB1が繰り返し実行される。そして、何かのコマンドが受信されると、ステップB2に進む。

ステップB2においては、受信されたコマンドがROM22に記憶した「暗号ダウンロードコマ

ンド」と一致するか否かが判断される。このステップB2で、YESと判断されるとステップB3に進む。

ステップB3では、暗号ダウンロードコマンドの後に送信されてくる暗号データをRAM23にセーブし、ステップB14に進む。

ステップB14において、結果OKを示すデータをCPU20に内蔵された送信バッファ（図示せず）にセットし、次のステップB17により送信バッファの内容をプリペイドカード端末装置に送信する。ステップB17の終了後はステップB1に戻る。

また、ステップB2でNOと判断された場合はステップB4に進む。ステップB4では、受信されたコマンドがROM22に記憶した「読み込みコマンド」と一致するか否かが判断される。このステップB4で、YESと判断されるとステップB5に進む。

ステップB5では、RAM23の暗号データエリアが正常か否かが判断される。ステップB5で

暗号データエリアが正常である場合はステップB6に進み、暗号データエリアがクリアされて正常でなければステップB16に進む。

ステップB6においては、暗号ルーチンをROM22から読み出し、RAM23に記憶された暗号データに基づいてプリペイドカードから読み出した残高データを復号化する。

ステップB7では、復号化された残高データをCPU20の送信バッファにセットし、次のステップB17により送信バッファの内容をプリペイドカード端末装置に送信する。ステップB17の実行後はステップB1に戻る。

次のステップB8により、受信されたコマンドがROM22に記憶した「書き込みコマンド」と一致するか否かが判断される。このステップB8で、YESと判断されるとステップB9に進む。

ステップB9においては、ステップB5と同様に、RAM23の暗号データエリアが正常か否かが判断される。ステップB9で暗号データエリアが正常であればステップB10に進み、正常でな

ければステップB 1 6に進む。

ステップB 1 0において、暗号ルーチンをROM 2 2から読み出し、RAM 2 3に記憶された暗号データに基づいてプリペイドカード端末装置から送信された残高データを暗号化する。

ステップB 1 1では、暗号化された残高データをリーダ・ライタメカニズム 2 1によりプリペイドカードに書き込み、ステップB 1 4に進む。

ステップB 1 4においては、結果OKを示すデータをCPU 2 0に内蔵された送信バッファにセットする。次のステップB 1 7では送信バッファの内容をプリペイドカード端末装置に送信し、ステップB 1に戻る。

また、上記ステップB 8でNOと判断された場合はステップB 1 2に進む。ステップB 1 2においては、受信されたコマンドがROM 2 2に記憶した「エジェクトコマンド」と一致するかが判断される。このステップB 1 2で、YESと判断されるとステップB 1 3に進み、リーダ・ライタメカニズム 2 1が作動してプリペイドカードが

外部に排出される。ステップB 1 3の実行後は、上述と同様に、ステップB 1 4、B 1 7が実行される。

しかして、ステップB 1 2でNOと判断される場合は、プリペイドカード端末装置から正常でないコマンドが送信されたことになるので、ステップB 1 5に進み、RAM 2 3の暗号データエリアをクリアしてプリペイドカードリーダ・ライタ 1 7を使用不可とする。

次のステップB 1 6では、暗号データが正常でないことを示す暗号NG情報をCPU 2 0の送信バッファにセットする。ステップB 1 7においては、上述と同様に送信バッファの内容をプリペイドカード端末装置に送信し、ステップB 1に戻る。

従って、ステップB 1 5によりRAM 2 3に記憶された暗号データがクリアされた後は、ステップB 5、B 9が実行された時に夫々NOと判断されるので、プリペイドカードに記録されたデータの復号化も暗号化もできず、プリペイドカードが不正に発券されることを防止できる。

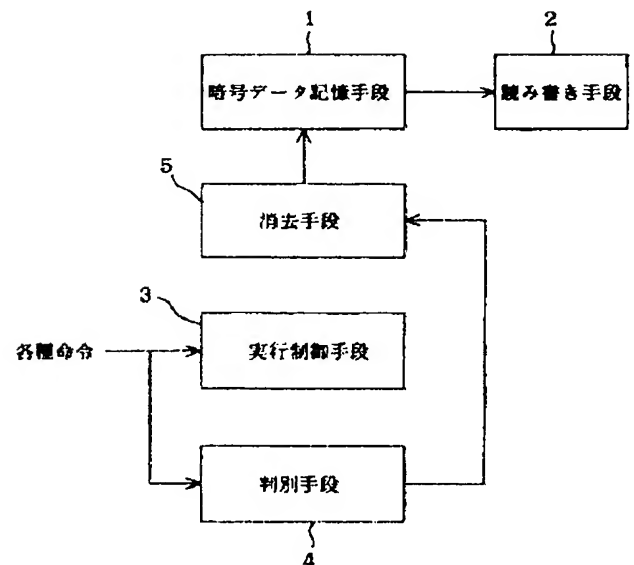
〔発明の効果〕

以上詳述したように、この発明によればプリペイドカードリーダ・ライタが盗難にあい、プリペイドカードに対して不正にデータを書き込もうとしても、異なった命令が指示された際に暗号データが消去されるので、プリペイドカードに正規のデータを書き込めず、プリペイドカードが不正に発券されることを防止できる。

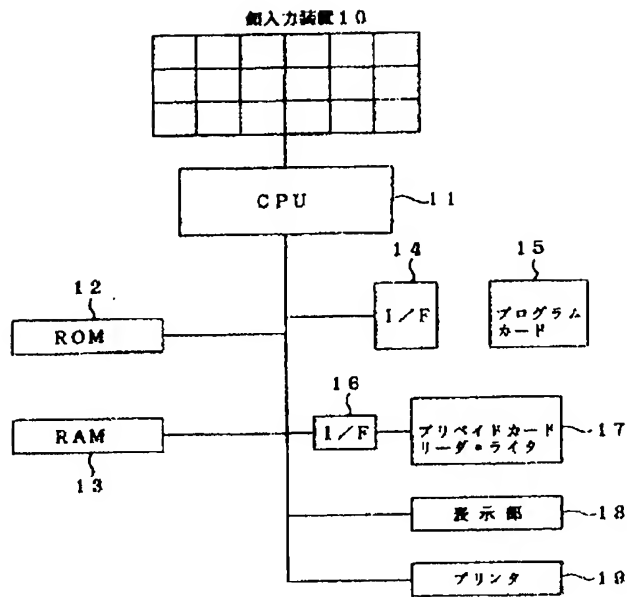
4. 図面の簡単な説明

図面は実施例を示すもので、第1図は本発明の機能ブロック図、第2図はプリペイドカード端末装置の回路構成を示すブロック図、第3図はプリペイドカードリーダ・ライタの回路構成を示すブロック図、第4図および第5図は動作を示すフローチャートである。

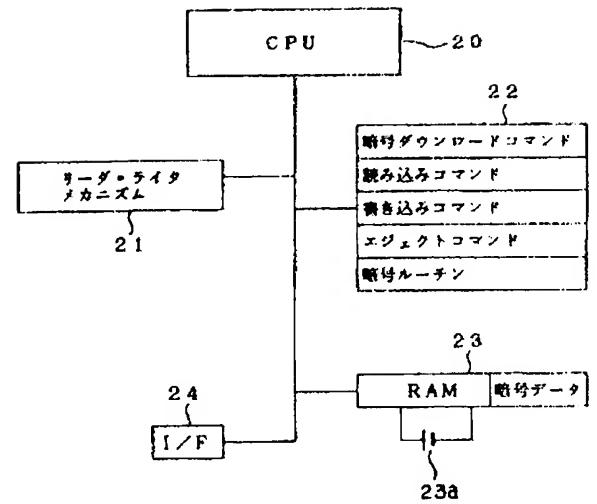
1…暗号データ記憶手段、2…読み書き手段、3…実行制御手段、4…判別手段、5…消去手段、20…CPU、21…リーダ・ライタメカニズム、22…ROM、23…RAM。



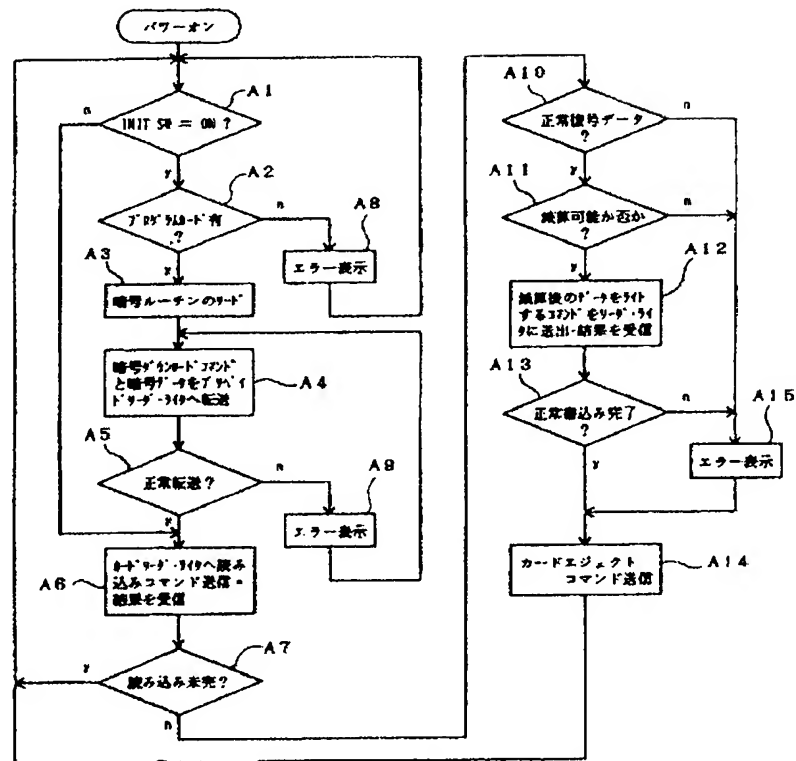
第1図



第 2 図



第 3 図



第 4 図

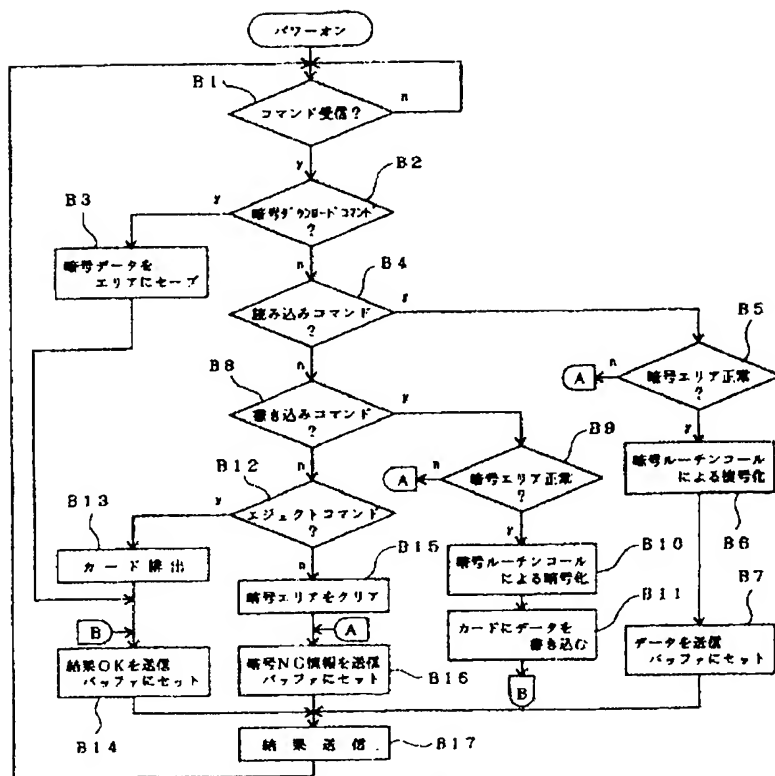


図 5